BSTZ No. 042390P13128
Express Mail No. EL802886783US

UNITED STATES PATENT APPLICATION

FOR

# EFFICIENT PEER TO PEER DISCOVERY

Inventor

Chandrashekar R. Padala



Prepared by:

Blakely, Sokoloff, Taylor & Zafman LLP
12400 Wilshire Boulevard, Suite 700
Los Angeles, California 90025
(714) 557-3800

# EFFICIENT PEER TO PEER DISCOVERY

## Field

The invention pertains generally to networks. More particularly, the invention relates to a more efficient discovery method for peer-to-peer communications across different networks.

## Background

In modern computer networks, computers (source computers) that seek to communicate with other computers (destination computers), also known as peer-to-peer communications, should be able to determine the address of the destination computer. Typically, a source computer has the name of the destination computer but does not have the destination address (binding information) necessary to communicate with the destination computer directly.

There are a few types of name-to-address resolution service models for networks supporting peer-to-peer communications. One such name-to-address resolution scheme uses a server to maintain a list of all peer contact or binding information (e.g., a name-to-address index), usually an Internet Protocol (IP) address. The disadvantage of this architecture is that it suffers from poor scalability and reliability. That is, as the network grows the list of peer addresses that is maintained becomes increasingly large. This inhibits efficient network communications. Because this approach relies on a server to maintain and provide peer addresses, this creates a large load on the server and exposes the network to a single point of failure. Additionally, delays in discovering new peers in the network is a source of unreliable communications.

One example of the server-centered name-to-address resolution service describe above is the World Wide Web (WWW) Domain Name Server (DNS) system.

Another service model relies solely on communications between peers to resolve peer names and contact binding information. That is, broadcast messages and/or other types of notification schemes may be employed to inform peers about contact binding information for other peers. This model, typically referred to as pure peer-to-peer approach, has the disadvantage of increasing network traffic and being less reliable as network traffic increases.

## BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a block diagram illustrating a network architecture with a typical peer address discovery scheme.

Figure 2 is a block diagram illustrating one embodiment of the multi-network name-to-address resolution aspect of the invention.

Figure 3 is a block diagram illustrating one embodiment of multi-network name-to-address resolution relationships according to one aspect of the invention.

Figure 4 is a block diagram illustrating various multi-network name-to-address resolution relationships at different hierarchical levels according to one embodiment of the invention.

Figure 5 is a flow diagram illustrating one method of sharing name-to-address resolution resources across multiple networks according to one embodiment of the invention.

## DETAILED DESCRIPTION

In the following detailed description of the invention, numerous specific details are set forth in order to provide a thorough understanding of the invention. However, the invention may be practiced without these specific details. In other instances well known methods, procedures, and/or components have not been described in detail so as not to unnecessarily obscure aspects of the invention.

Throughout this description, the term 'address' generally refers to any contact or binding information necessary for a first peer to communicate with another peer. The term 'peer' generally refers to various devices including a processing device/unit, computer systems, and data storage devices. The term 'server' generally refers to any computer or device which manages, maintains, and/or facilitates communications to and/or from other computers. As employed in the description and claims, the term 'name-to-address index' is used interchangeably to generally refer to any address resolution resource that may be employed. Thus, the term 'index' should includes hash tables, look-up lists, and any other address resolution resource or method.

In the accompanying figures, dashed lines are often used to indicate communications between devices and do not necessarily indicate a physical interface or coupling. Also, the label for each device (block) appears boxed or framed within the device.

The invention provides a system, method, and device for quick and efficient peer-to-peer discovery (name-to-address resolution) across a multi-network.

Referring to Figure 1, one embodiment of a typical enterprise network is illustrated. An enterprise server (ES) serves as the host for name-to-address information for peers under it. In this illustration, the ES hosts the peer name-

to-address list/index for two networks, business unit #1 (BU1) network and business unit #2 (BU2) network. Each network comprises one or more peers (e.g., P1, P2, P3, P4, and PN for the BU1 network and X1, X2, X3, X4, and XN for the BU2 network - where N denotes a positive integer). Each of the business unit servers (e.g., BU1 and BU2) typically maintains an index of local peer addresses. For example, BU1 maintains a list of the peer addresses for the peers in its network (e.g. P1-PN). Similarly, business unit server BU2 maintains the peer addresses for the peers in its local network (e.g. X1-XN).

Typically, a first peer that seeks to communicate with another peer in its network first obtains the address for the other peer. For example, in Figure 1 if P1 wishes to communicate with P4 it first obtains its address from the business unit (BU1) server for the local network. Since BU1 is the address server for the local network, it maintains the address for peer P1 through PN, including P4. Thus, BU1 will be able to provide P1 with the address for P4. Upon receipt of the P4 address, P1 will be able to communicate (send messages) with P4.

In one implementation, once a peer obtains the address information for another peer it stores it for future reference. Thus, a peer may maintain and index or list of one or more addresses. For example, P1 maintains a list of other peer addresses including, P2 and P3. Similarly, peer P2 maintains the addresses for peers P3 and P4, peer P3 maintains the addresses for peers P4 and P1, peer P4 maintains the addresses for P2 and P3, and PN maintains the address for P1.

In one embodiment, a peer may save only the last n peer addresses of the peers with which it communicated, where n is a positive integer. Peers may also maintain other addresses such as the local business unit server (e.g. BU) and enterprise server (e.g. ES) to expedite network communications.

When a peer operating in a first network seeks to communicate with another peer operating in a second network it typically obtains the other peer's address from a server common to both networks. In a hierarchical network this means going up the hierarchy until a computer (server) is found which spans both networks. For example, when peer XN in the BU2 network seeks to communicate with peer P1 in the BU1 network, it first obtains its address. Peer XN first tries to obtain the address for P1 from its local server BU2. Since P1 is in another network, BU2 is unable to provide the address, and the request fails. Peer XN then goes up one level to the enterprise server ES and request the address for P1. Since ES acts as the name server host for peer addresses in both the BU1 and BU2 networks (it is common to both networks), it maintains address information for peers in both networks, including P1. Thus, ES would respond to XN's request with the address information for P1.

The address discovery system described above and illustrated in Figure 1 has the disadvantage of relying on a single server ES to permit peer-to-peer communications across two networks (e.g. BU1 network and BU2 network). As noted above, reliance on a single server for inter-network communications causes traffic congestion and is susceptible to a single point of failure.

One aspect of the invention provides a scheme to permit peer-to-peer communications between networks without reliance on a higher level server. A relationship is established between servers, each in different networks, to permit address information discovery or exchange (name-to-address resolution) for peers in one or both of the networks.

Referring to Figure 2, a group of networks each managed by a business server (e.g. BU1, BU2, and BU3) and all served by a single higher level server (e.g. ES) is illustrated. Like the network describe in Figure 1, if peer XN in network

BU3 seeks to communicate with P1 in network (BU1), it contacts the common higher level server ES to obtain its address.

According to one embodiment of the invention, a relationship is established between business unit servers BU1 and BU2 such that a name-to-address resolution resources can be shared from one network to the other may be established without reliance on the higher level server (ES). For example, if peer P1 in the BU1 network seeks to communicate with peer A1 in the BU2 network it requests its address from its local server BU1 as usual. Because a relationship has been established between servers BU1 and BU2 (indicated by the direct bi-directional dashed line between the two servers), server B1 is able to query server B2 to obtain the address for A1 and return it to the requesting peer P1. Thus, P1 is able to establish peer-to-peer communications without relying on the enterprise server ES for cross-network address resolution.

Once a peer has obtained the address information for another peer, either within its local network or in another network, it may store such address for later reference.

The address sharing relationship between two or more servers may be characterized as creating a 'common zone' across multiple networks. Common zones generally refer to logical groups of two or more networks which at some level share address resolution/discovery information without relying on higher level or common servers to do so. As used herein, common servers are servers which are at a higher level in the server hierarchy and span both of the networks.

A common zone creates a transparent address discovery interface. From the perspective of a peer in a first network, peers on other networks appear to be 'local' since there is no need to contact a higher level server to obtain its address.

While the illustration in Figure 2 depicts a common zone for peers of networks BU1 and BU2, common zone relationships are not limited to networks (or business units or servers) at the same hierarchical level. A common zone may be formed

between multiple networks at the same hierarchical level or networks at different hierarchical levels. For example, business server BU1 may form a common zone relationship with a network operating under X3 (in network BU3) to share name-to-address information and expedite address resolution for peer-to-peer communications. Additionally, a local server (e.g. BU1) may establish multiple independent common zones with other servers.

Another aspect of the invention enables access protection and restricted access to the peers on a given network. Unlike the typical DNS hierarchical architecture, where peer access may not be individually restricted to certain peers, common zone access according to the invention permits authorization-based access to peers across multiple networks. Only peers in the same common zone (e.g., BU1 and BU2) are allowed to discover an address without having to query a higher level server common to both networks (e.g, ES). In one implementation, relationships between local servers (or servers within a common zone) permit restricting access to authorized peers only.

According to one implementation, a local server (e.g. BU2) may require a password or other authentication information before permitting an address discovery or sharing relationship to be established with another server (e.g. BU1) at the same hierarchical level. In other implementations, each server has a list of local servers with which it is allowed to share peer address information. A server may then check this list to determine if it may respond to an address information request from another server.

Derivative or indirect address resolution via the common zone relationships may be permitted or restricted depending on the implementation. Derivative or indirect address resolution may occur where one server maintains two common zone relationships with two other servers. For example, as illustrated in Figure 3, server BU2 maintains a common zone

relationship A with BU1 and a common zone relationship B with BU3. However, there is no direct common zone relationship between BU1 and BU3. Thus, BU2 may enable or prohibit common zone address discovery from BU1 to BU3 depending on the application.

In one implementation, server BU2 may deny an address request from a first peer in the BU1 network (e.g. P1) for an address of a second peer in the BU3 network (e.g. X1). In another implementation, server BU2 may provide the address information to a peer in the BU1 network (e.g. P1) seeking to communicate with a peer in the BU3 network (e.g. X1).

Figure 4 illustrates yet another implementation of the invention where a common zone relationship is created across two enterprise networks. For example, a name-to-address sharing relationship may be created between ES1 and ES2 such that shared peer address discovery may be implemented. For instance, a peer X5 within network BU4 may seek to communicate with a peer A4 within network ES1. First, X5 requests A4's address from its local server BU4. If such request fails because BU4 does not have access to A4's address, X5 requests the address from the next higher level server ES2. Since ES2 has an address sharing relationship (relationship A) with ES1, it is able to obtain the address and respond to the request. Moreover, the address sharing relationship between ES1 and ES2 does not prevent other direct address sharing relationships from being established. For example, a direct address sharing relationship (relationship B) may be established between BU2 and BU3, each on different networks ES1 and ES2 respectively. Thus, when peer Z1 in network BU3 seeks to communicate with peer A4 in network BU2, then server BU3 may directly query server BU2 to obtain A4's address.

Referring to Figure 5, according to one embodiment of the invention a server receives a request from a first peer for the binding information or address of a second peer 502. The server checks its local index to resolve the requested address

504. If the address is found 504, then the server returns the address to the first peer 508. If the address is not found 504, then the server directly checks with servers for other networks within its common zones 510 to try to resolve the address request. If the second peer belongs to one of the other networks within the common zone, the address will be resolved and returned to the first peer 512 and 508. If the address is not found, then the server returns an address invalid or address not found message to the first peer 514.

While certain exemplary embodiments have been described and shown in the accompanying drawings, it is to be understood that such embodiments are merely illustrative of and not restrictive on the broad invention, and that this invention should not be limited to the specific constructions and arrangements shown and described. Additionally, it is possible to implement the invention or some of its features in hardware, programmable devices, firmware, software or a combination thereof. The invention or parts of the invention may also be embodied in a processor readable storage medium or machine-readable medium such as a magnetic, optical, or semiconductor storage medium.